IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

DONNA CURLING, et al. **Plaintiffs,** **vs.** **BRAD RAFFENSPEGER, et al.** **Defendants.**	**CIVIL ACTION FILE NO.: 1:17-cv-2989-AT**

DECLARATION OF RICHARD DEMILLO

RICHARD DEMILLO declares, under penalty of perjury, pursuant to 28 U.S.C. §1746, that the following is true and correct:

1. My name is Richard DeMillo. I am a tenured Full Professor at the Georgia Institute of Technology (Georgia Tech), where I hold the Charlotte B. and Roger C. Warren Chair in Computing. I received my Ph.D. from Georgia Tech in 1972 and have held positions of responsibility in academia, the federal government, and industry. I have held technical and senior executive positions and have published over a hundred books, patents, and articles related to cybersecurity. My work has been cited over 15,000 times, and several have been republished in collections of the most important contributions to computer science. I am a fellow of the Association for

Computing Machinery and the American Association for the Advancement of Science in recognition of my work in cybersecurity, which has been my focus for most of my career. The attached resume describes these positions, board memberships, and advisory roles in Government and industry. (Exhibit 1) My most recent assignment at Georgia Tech was to launch a new School of Cybersecurity and Privacy (SCP), ranked by the U.S. News & World Report as the Number 1 cybersecurity department in the country.

2. I have consulted pro bono with the Plaintiff's counsel in the present lawsuit and previously submitted declarations to explain and clarify technical matters related to this lawsuit. Although this declaration is unrelated to my previous statements, I stand by my earlier declarations.
3. Under a signed protective order, I have reviewed the redacted and unredacted versions of a report ("the Halderman Report") by Prof. J. Alex Halderman filed with the Court describing certain vulnerabilities inherent in the Dominion voting system currently in use in the State of Georgia, and in some other jurisdictions
4. I understand that the Halderman Report has been sealed since its issuance, and I further understand that the decision to keep the report secret was motivated by a concern that public disclosure of Dominion voting system vulnerabilities detailed in the Halderman Report would educate potential

threat actors in ways to exploit those weaknesses, thereby further degrading the system's security.

5. It is an established principle of cybersecurity that such a concern is misplaced and that the potential risks of disclosing vulnerabilities to hackers are vastly outweighed by the security enhancements that can only be achieved by prompt, responsible public disclosure of vulnerabilities. In effect, the natural inclination to insist on strict secrecy undermines system security. The reasoning behind this conclusion is explained below:

    a. Halderman's reports were prepared and disclosed following a CISA process known as Responsible Vulnerability Disclosure which privately reports vulnerabilities to the parties involved so a prompt fix can be developed before the vulnerability is made public.

    b. Responsible Vulnerability Disclosure is a security-enhancing practice described by security agencies, standards bodies, and standard textbooks, such as:

        i. The Computer Emergency Response Department of the Software Engineering Institute at Carnegie Mellon University, a Federally Funded Research and Development Center chartered by the U.S. Department of Defense[1]

[1] https://resources.sei.cmu.edu/asset_files/specialreport/2017_003_001_503340.pdf

ii. The Cybersecurity and Infrastructure Security Agency (CISA), an agency of the U.S. Department of Homeland Security[2]

iii. The International Standards Organization (ISO), an independent, non-governmental international organization with a membership of 168 national standards bodies.[3]

iv. Security in Computing (4th Edition) by Charles P. Pfleeger and Shari Lawrence Pfleeger, Prentice Hall, 2017, pp. 675-6

v. Disclosure of Security Vulnerabilities: Legal and Ethical Issues by Alana Maurushat, Springer, 2013

c. Contrary to some people's belief, Responsible Vulnerability Disclosure does not involve keeping a vulnerability secret. As described in all these sources, security is degraded if the vulnerability is kept secret. Secrecy prohibits information sharing, vulnerability mitigation, and user awareness of a threat all of which are critical steps in enhancing system security. Among other benefits of public disclosure is the spotlight on vendors and software developers that promotes prompt fixing of a software defect or vulnerability.[4]

---

[2] https://www.cisa.gov/vulnerability-disclosure-policy-template
[3] https://www.iso.org/standard/72311.html
[4] https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html

d. The information theoretical underpinnings of vulnerability disclosure are summarized in Kirchoff's Principle, which states that, except for cryptographically secured information, system developers should never assume they have secret system knowledge unknown to attackers. Vulnerabilities exist whether or not they are disclosed. Once discovered, there is no theoretical advantage to assuming their existence is not known to bad actors.

e. Keeping Professor Halderman's (redacted) report under seal undermines the solid foundation for the concept of Responsible Disclosure which is critical to enhancing cybersecurity. Doing so degrades cybersecurity by unnecessarily prolonging the resolution of security issues, discouraging collaboration among security researchers and organizations, and eroding both public trust, and a culture of security awareness.

f. Responsible Disclosure does not give a free license to publicize detailed information that would make an attacker's job easier, and the Court is correct in restricting access to some of the details in the unredacted version of the Halderman Report. This specific information that should not be made public has already been identified by CISA and Professor Halderman. Nothing in my declaration should

be interpreted as advocating that such details be released to the general public.

6. In the special case of voting system cybersecurity vulnerabilities, it is particularly important that state and local election officials across the nation have responsible accurate expert explanations of serious vulnerabilities, such as the Halderman Report, promptly available to them in time to plan to mitigate the elevated risk to 2024 elections caused by Georgia's voting system breaches in 2021. Officials across the nation are bombarded by disinformation about voting system issues from irresponsible actors. They will be naturally hesitant to act to make needed changes without expert validated information such as the Halderman Report, validated by CISA. Withholding expert information from these officials responsible for protecting the nation's election infrastructure, and the technical advisors on whom they rely, serves to retard mitigation to the current serious cybersecurity concerns.

7. I understand that responsible vulnerability disclosure may be confused with the unauthorized release of executable images that occurred in Coffee County and possibly other jurisdictions. Making public the executable images of election software Georgia's degraded system security, was highly irresponsible and unrelated to Responsible Disclosure. The Coffee County

incident did not disclose vulnerabilities. It simply made it much easier to discover exploitable errors and weaknesses. Publishing executable software images without notifying the vendor provides an inexpensive way for any bad actor to use off-the-shelf tools to experiment with and reverse engineer software, a critical step in probing the system to discover previously unknown weaknesses and vulnerabilities. Those vulnerabilities could be exploited before Dominion or election officials had time to fix the weaknesses. Incidents such as the statewide breach allegedly occurring via Coffee County are the opposite of responsible disclosure. The information released in Responsible Disclosure is limited to understanding a weakness already discovered and fixed. While there is a small potential risk of disclosing exploitable information, that risk is outweighed by the security-enhancing features of responsible disclosure.

In summary: the potential risks of further disclosing vulnerabilities to bad actors are far outweighed by the benefits of responsible disclosure in improving voting system cybersecurity.

Executed on this date, May 15, 2023

Richard DeMillo

EXHIBIT

1

Richard A. DeMillo

Curriculum Vita

Present Position

- Georgia Institute of Technology, Atlanta GA 30332
  - Charlotte B. and Roger C. Warren Professor of Computing
  - Professor of Management,

Education

- BA, Mathematics, 1969, College of St. Thomas, St. Paul Minnesota
- Ph.D., Information and Computer Science, 1972, Georgia Institute of Technology, Atlanta, Georgia

Professional Experience

2020-Present	Interim Chair School of Cybersecurity and Privacy Georgia Institute of Technology Atlanta, Georgia 30332
2020-Present	Managing Director Gtatrium, LLC A Subsidiary of Georgia Advanced Technology Ventures
2015-Present	Charlotte B. and Roger C. Warren Professor of Computing Georgia Institute of Technology Atlanta, GA 30332
2010-2020	Director, Center for 21st Century Universities Georgia Institute of Technology Atlanta GA 30332
2013-2014	Distinguished Chief Scientist Qatar Computing Research Institute Qatar Foundation Doha, Qatar
2002-Present (On Leave 2013-2014)	Professor of Management John P. Imlay Dean of Computing (2002-2009) Director, Georgia Tech Information Security Center (2002-2004) Georgia Institute of Technology Atlanta, Georgia 30332
2000-2002	Chief Technology Officer Vice President Hewlett-Packard Company 3000 Hanover Street Palo Alto, CA 94303
2000	General Manager Internet Systems Group Telcordia Technologies (Formerly Bellcore) 445 South Street Morristown, NJ 07960
1994-2000	Vice President and General Manager Information and Computer Sciences Research Telcordia Technologies (Formerly Bellcore) 445 South Street

	Morristown, NJ 07960
1994	Visiting Professor Department of Electronics and Informatics University of Padua Padua, Italy
1989-91	Director Computer and Computation Research Division National Science Foundation 1800 G Street NW Washington, DC
1987-96	Professor of Computer Science and Director Software Engineering Research Center Purdue University West Lafayette, Indiana
1985-87	Director Software Engineering Research Center Georgia Institute of Technology Atlanta, Georgia
1984-87	Assistant Director for Research School of Information and Computer Science Georgia Institute of Technology Atlanta, Georgia
1981-87	Professor of Information and Computer Science School of Information and Computer Science Georgia Institute of Technology Atlanta, Georgia
1976-81	Associate Professor of Information and Computer Science School of Information and Computer Science Georgia Institute of Technology Atlanta, Georgia
1972-76	Assistant Professor Department of Electrical Engineering and Computer Science University of Wisconsin, Milwaukee Milwaukee, Wisconsin
1969-72	Research and Teaching Assistant School of Information and Computer Science Georgia Institute of Technology Atlanta, Georgia
1969-71	Research Assistant Los Alamos National Laboratory Los Alamos, New Mexico

Research and Consulting Experience

Rich has been a consultant to many major corporations and other organizations. Detailed descriptions of recent consultantships are available upon request:

Board Memberships

Rich has been a board member and director of many public and private corporations, foundations and philanthropic organizations. Detailed descriptions of recent board memberships are available upon request:

Professional Recognition

ANAK, Outstanding Faculty Award (2106)

Annual Achievement Award of the Association for Educational Communications and Technology (2019)

American Publishers Association Best Book Award (Education, 2016)

Inaugural Fellow of the Lumina Foundation

Fellow of the Association for Computing Machinery

Fellow of the American Association for the Advancement of Science

Panels and Advisory Positions

1983:	Secretary of Defense Blue Ribbon Panel (The Eastman Panel) to Define the Software Engineering Institute (SEI)
1983-1985:	IBM Software Tools Advisory Board
1984:	Congressional Office of Technology Assessment Panel on Research Directions in Software Engineering.
1987:	National Research Council Committee on Computer Security
1993-1996:	National Research Council committee on Statistical Methods in Software Engineering
1992-1993:	FAA VSCS Independent Fault Analysis Team
1995:	National Research Council committee on Commercial Software Practices in Defense Software
1995-2000:	Princeton University Computer Science Advisory Committee
1998-2000:	Advisory Board of the College of Computing, Georgia Tech
2000-3:	Georgia Tech Advisory Board
2001-2005:	Advisory Board of the Johns Hopkins University Computer Sciences Department
2003-2005:	National Research Council Committee on Telecommunications Research
2004-2005:	National Research Council Committee on Network Science and the Army's Future Needs
2005	Defense Science Board Committee on Security of Software
2010-2013	Strategic Advisory Committee (Chair) Qatar Computing Research Institute
2012	AMA Advisory Board on Medical Education
2012-2016	World Economic Forum Global Action Council on the Future of Universities
2012-2015	Pacific Northwest National Laboratories National Security Advisory Council
2012-2016	Western Governors University Advisory Board
2013-2016	Singapore Institute of Technology and Design Advisory Board
2015	IEEE Computer Society, Research Advisory Board
2019	Michigan Commission on Election Security, Department of State, State of Michigan
2020	US Department of Education, Education Blockchain Initiative

Editorships

1990-96	Series Editor, *Software Science and Systems*, Plenum Publishing Company

1989-96	Editorial Board, *ACM Transactions on Software Engineering and Methods*
1988-94	Editorial Board, *IEEE Transactions on Software Engineering*
1985-87	Editorial Board, *Information and Control*
1982-85	Editorial Board, *ACM Transactions on Mathematical Software*

Biographical

- American Men and Women of Science
- Who's Who in America
- Who's Who in the World

Professional Societies

- Association for Computing Machinery
- American Mathematical Society
- Mathematical Association of America
- Society for Industrial and Applied Mathematics
- American Association for the Advancement of Science
- Association for Symbolic Logic
- IEEE

Rich has served on numerous program committees for professional meetings. In addition, Rich has served as Chairman or Program Chairman for the following annual conferences

- 15th International Conference on Software Engineering, 1993
- ACM SIGSOFT Annual Symposium, 1989 (Testing, Analysis and Verification)
- ACM Computer Science Conference, 1988
- ACM Symposium on Theory of Computing, 1984
- NSIA Conference on Test and Evaluation, 1983
- ACM Symposium on Principles of Programming Languages, 1982
- First IEEE Symposium on Security and Privacy, 1981

Publications

Books

- R. A. DeMillo, *After the Revolution: How a Global Pandemic and the Changing Face of Work Transformed Colleges and Universities, In preparation*
- R. A. DeMillo, *Revolution in Higher Education: How A Small Band of Innovators will Make College Accessible and Affordable*, MIT Press 2015 (foreword by Amb. Andrew J. Young)
- R. A. DeMillo, *Abelard to Apple: The Fate of American Colleges and Universities*, MIT Press, 2011.
- R. A. DeMillo and J. R. Rice, Editors, *Studies in Computer Science*, Plenum Press 1994

- R. A. DeMillo, W. M. McCracken, R. J. Martin, J. F. Passafiume, *Software Testing and Evaluation*, The Benjamin-Cummings Publishing Company, Inc. 1986.
- G. I. Davida, R. A. DeMillo, D. P Dobkin, M. A. Harrison, R. J. Lipton, *Applied Cryptology, Cryptographic Protocols, and Computer Security*, American Mathematical Society (Applied Mathematics Series), 1984, American Mathematical Society. (Also: Indonesian edition, translated by Pangeran Sianipar, 1994)
- R. A. DeMillo, D. P. Dobkin, A. K. Jones, and R. J. Lipton, Editors, *Foundations of Secure Computation*, Academic Press, 1978

Special Publications

- Michigan Election Security Advisory Commission Report and Recommendations, October 2020 ESAC_Report_Recommendations_706522_7.pdf (michigan.gov)
- Deliberate Innovation, Lifetime Education: Report of the Commission on Creating the Next In Higher Education," Atlanta Georgia 2018 https://dx.doi.org/10.2139/ssrn.3753524
- "Statistics and Software Engineering", National Academy of Sciences, National Research Council Committee on Statistics, Document Number, 1996, Washington, DC.
- "Report of the Voice Switching and Control System (VSCS) Independent Fault Tolerance Analysis Team (VIFTAT)," A Report to the Federal Aviation Administration, MITRE Report (January, 1993).
- "Computer and Information Security in the Department of Energy's Classified Environment" (U), National Academy of Sciences, National Research Council Committee on Computer Security Doc. No. 88-EEB-2, 1988, Washington, DC (Classified Report)
- R. A. DeMillo, "Operational Readiness of the Patriot Air Defense System Software"(U), Report to Director Operational Test and Evaluation, USDRE, 1985 (Classified Report)
- R. A. DeMillo, "Software Test and Evaluation Manual: Volume 1, Guidelines for the Treatment of Software in Test and Evaluation Master Plans", Sept., 1984. Issued by the Office of the Secretary of Defense as Attachment to Department of Defense Directive 5000.3 ("Test and Evaluation") DoDD 5000.3-M-3.
- "Software Testing", *Encyclopedia of Information and Computer Science, 3rd Edition*, Anthony Ralston
- "Observing the 2006 Presidential Elections in Venezuela: Final Report of the Technical Mission," The Carter Center, 2007
- "New Ecosystems in Higher Education and What They Mean for Accreditation and Assessment, in WASC Concept Papers, 2nd Series: The Changing Ecology of Higher Education and its Impact on Accreditation, March 2013, Western Association of Schools and Colleges, Accrediting Commission for Senior Colleges and Universities.
- "Governance for a New Era: A Blueprint for Higher Education Trustees," Project on Governance for a New Era, Benno Schmidt, Chairman, August 2014
- "Deliberate Innovation, Lifetime Education: Report of the Commission on Creating the Next In Education," March, 2018. Georgia Tech

Selected Recent Articles, Op-Ed and Opinion

"Georgia Voting Processes Should be Both Secure and Usable," with Michael Best and Ellen Zegura, Atlanta Journal and Constitution, March 13, 2021 Opinion: Ga. voting processes should be both secure and usable (ajc.com)

"Georgia's new voting machines aren't any more secure," Atlanta Journal-Constitution, August 24, 2019 https://www.ajc.com/news/opinion/opinion-new-voting-machines-aren-any-more-secure/oxfbdSoCpglUtuUCGGbrrK/

"Replace Georgia's Risky Touchscreen Voting Machines," Atlanta Journal-Constitution, July 27, 2018,https://www.ajc.com/news/opinion/opinion-replace-risky-touchscreen-voting-machines/IjncsjZgBylGqekhN7L3cJ/

"This Will Go On Your Permanent Record! How Blockchains Can Transform Colleges in a Networked World," The EvoLLLution, May 5, 2017, https://evolllution.com/programming/credentials/this-will-go-on-your-permanent-record-how-blockchains-can-transform-colleges-in-a-networked-world/

"The Human Element and the Power of Big Data in Higher Education." The EvoLLLution, March 25, 2017

"Georgia's Election System Can't be Trusted." Bloomberg View, December 18, 2017, https://www.bloomberg.com/view/articles/2017-12-18/georgia-s-election-system-can-t-be-trusted

"Election Hacking is Going to Happen. Here's What We Can Do Now to Protect Our Vote," (with Candice Hoke and Duncan Buell) USA Today, March 25, 2018, https://www.usatoday.com/story/opinion/2018/03/15/russian-election-hacking-what-we-can-do-now-protect-democracy-buell-demillo-hoke-column/393565002/

"Gatekeepers No More: Colleges Must Learn a New Role," The Chronicle of Higher Education, September 14, 2015, https://www.chronicle.com/article/Gatekeepers-No-More-Colleges/232975

Patents

D. Boneh, R. DeMillo and R. Lipton , "Method of using transient faults to verify the security of a cryptosystem" , Patent Number 6,965,673

Invited Talks, Keynotes

Rich is a frequent speaker at conferences and events. Details are available upon request

Papers and Book Chapters

1. J. Gough and R. A. DeMillo, "Towards an Ostensive Grammar I" *Eighth Annual Meeting of the Association for Computational Linguistics* (July 1970), Columbus, Ohio.
2. R. A. DeMillo, "An Application of an Ostensive Grammar to the Analysis of Existential Predicates", *Proceedings of the Southeastern Conference on Linguistics* (October 1970), Atlanta, Georgia.
3. L. Chiaraviglio and R. A. DeMillo, "On the Applicative Nature of Assignment", Georgia Institute of Technology Report Number GIT-ICS-71-1 (1971).
4. R. A. DeMillo, *Formal Semantics and the Logical Structure of Programming Languages,* Ph.D. Thesis, 1972, Georgia Institute of Technology, Atlanta, Georgia.
5. R. A. DeMillo, "Parallelism and Non-Determinism in the Lattice of Programs", *Record of the Computer Science Conference,* (February 1973), Columbus, Ohio.
6. R. A. DeMillo, "Constructing and Verifying Courses of Action in Robots," *Proceedings of MSAC-73,* (February 1973), Milwaukee, Wisconsin.
7. R. A. DeMillo and R. A. Northouse, "Autonomous Computing: Perspectives and Models for Artificial Intelligence," *Proceedings MSAC-74,* (February 1974), Milwaukee, Wisconsin.
8. R. A. DeMillo and K. Vairavan, "Parallel Scheduling of Programs in a Restricted Model of Computation", *Proceedings Sixth ACM Symposium on Theory of Computing,* (May 1974), Seattle, Washington.
9. R. A. DeMillo, "A Lattice Theoretic Interpretation of a Theorem by Patil," University of Wisconsin-Milwaukee Technical Report No. 75-6 (1975)
10. R. A. DeMillo, S. C. Eisenstat and R. J. Lipton, "The Complexity of Control and Data Structures", *Proceedings Seventh Annual Symposium on Theory of Computing*, Albuquerque, New Mexico (May 1975), pp. 186-193.

11. R. A. DeMillo, S. Amoroso and M. Wolfe, "Primitives for Tactical Real-Time Control Languages based on Simula 67 II: Design and Implementation Considerations", CENTAC Report No. 58, US Army Electronics Command, Fort Monmouth, NJ (1975).

12. R. A. DeMillo, S. Amoroso and M. Wolfe, "Primitives for Tactical Real-Time Control Languages based on Simula 67 I: General Language Considerations", CENTAC Report No. 50, US Army Electronics Command, Fort Monmouth, NJ (1975).

13. R. A. DeMillo, "Nondefinability of Certain Semantic Properties of Programs", *Notre Dame Journal of Formal Logic*, Vol. 16, No. 4, (1975), pp. 583-590.

14. R. A. DeMillo, S. C. Eisenstat and R. J. Lipton, "Space-Time Tradeoffs in Structured Programming", *Proceedings 1976 Johns Hopkins Conference on Information Systems and Sciences*, Baltimore, Maryland, (March, 1976), pp. 240-245.

15. R. A. DeMillo, S. C. Eisenstat and R. J. Lipton, "Programming Language Studies I: The Power of Control and Data Structures" University of Wisconsin-Milwaukee Technical Report No. 76-13 (1976)

16. R. A. DeMillo, S. C. Eisenstat and R. J. Lipton, "Can Structured Programs be Efficient", *SIGPLAN Notices*, Vol. 11, No. 10, (October, 1976), pp. 10-18.

17. R. A. DeMillo, S. C. Eisenstat and R. J. Lipton, "Space and Time Hierarchies for Classes of Control and Data Structures", *Journal of the ACM*, Vol. 23, No. 4 (October, 1976), pp. 720-730.

18. R. A. DeMillo, S. C. Eisenstat, and R. J. Lipton, "Space-Time Tradeoffis in Structured Programming: Reducible Flowgraphs (Abstract Only), Computer Science Conference, 1976.

19. K. Vairavan and R. A. DeMillo, "On the Computational Complexity of a Generalized Scheduling Problem", *IEEE Transactions on Computers*, Vol. C-25, No. 10 (October, 1976), pp. 720-732. This paper has been reprinted under the same title in *Distributed Computing: Concepts and Implementations*, edited by Paul McEntire, John G. O'Reilly and Robert E. Larsen, published by IEEE Press (1984).

20. R. A. DeMillo, R. J. Lipton and A. J. Perlis, "Social Processes and Proofs of Theorems and Program", *6th ACM Symposium on Principles of Programming Languages* (January 1977) Santa Monica, California, pp. 245-262 [See main entry number [40] below].

21. R. A. DeMillo, K. Vairavan and E. Sycara-Cyranski, "A Study of Schedules as Models of Parallel Computation", *Journal of the ACM*, Vol. 24, No. 4 (October, 1977), pp. 544-565.

22. R. A. DeMillo, "Some Applications of Model Theory to the Metatheory of Program Schemata", *Notre Dame Journal of Formal Logic",* Vol. 18, No. 3, 1977, pp. 489-495.

23. R. A. DeMillo, S. C. Eisenstat, and R. J. Lipton, "Preserving Average Proximity in Arrays" *Communications of the ACM",* Vol. 23, No. 3, (March 1978), pp. 228-230.

24. R. A. DeMillo and R. J. Lipton, "A Constructive Generalization of the Borel-Cantelli Lemma with Applications to the Complexity of Infinite Strings", *Mathematical System Theory",* Vol, 13, 1979, pp. 95-104.

25. R. A. DeMillo, D. P. Dobkin and R. J. Lipton, "Combinatorial Inference", *Proceedings 1977 Allerton Conference on Communication, Control and Computing* [Also appears in R. DeMillo et al (editors), *Foundations of Secure Computation*, Academic Press, 1978, pp. 27-38.

26. R. A. DeMillo, D. P. Dobkin and R. J. Lipton, "Even Data Bases that Lie can be Compromised", *IEEE Transactions on Software Engineering",* Vol SE-4, No. 1 (January, 1978), pp. 71-74.

27. B. H. Barnes, G. I. Davida, R. A. DeMillo, L. H. Landweber, H. Stone, "Theory in the Computer Science and Engineering Curriculum", *IEEE Computer",* Vol. 18, No. 12 (December, 1977), pp. 106-108.

28. R. A. DeMillo, R. J. Lipton and L. G. McNeil, "Proprietary Software Protection" in R. A. DeMillo et al (editors), *Foundations of Secure Computation",* Academic Press, 1978, pp. 115-132.

29. R. A. DeMillo and D. P. Dobkin, "Foundations of Secure Computation", in R. A. DeMillo et al (editors), *Foundations of Secure Computation",* Academic Press, 1978, pp. 1-3.

30. R. A. DeMillo, S. C. Eisentat and R. J. Lipton, "On Small Universal Data Structures and Related Combinatorial Problems", *Proceedings 1978 Johns Hopkins Conference on Information Systems and Sciences",* March, 1978, Baltimore, Maryland, pp. 416-428.

31. R. A. DeMillo, R. J. Lipton and F. G. Sayward, "Program Mutation as a Tool for Managing Software Development", *Proceedings of the 32nd Annual Meeting of the American Society for Quality Control",* May 1978, Chicago, Illinois, pp. 326-348.

32. T. A. Budd, R. A. DeMillo, R. J. Lipton, and F. G. Sayward, "The Design of a Prototype Mutation System for Program Testing", *Proceedings 1978 National Computer Conference",* pp. 623-627.

33. R. A. DeMillo and R. J. Lipton, "A Probabilistic Remark on Algebraic Program Testing", *Information Processing Letters*, Vol. 7, No. 4 (June, 1978) pp. 193-195.

34. R. A. DeMillo, R. J. Lipton and F. G. Sayward, "Discussion of Software Testing Issues", in P. Wegner (editor) *Research Directions in Software Technology*", MIT Press (1978) pp. 408-413.

35. R. A. DeMillo, R. J. Lipton and F. G. Sayward, "Hints on Test Data Selection: Help for the Practicing Programmer", *Computer*, Vol. 11, No. 4 (April, 1978) pp. 34-43. This paper has been reprinted several times under the same title. It has recently appeared in Tutorial*: Software Testing and Validation Techniques* edited by Edward Miller and William Howden, IEEE Computer Society Press (1981).

36. R. A. DeMillo, R. J. Lipton and A. J. Perlis, "Response to Dijkstra's On a Political Pamphlet from the Middle Ages", *Software Engineering Notes*, Vol. 3, No. 2 (April, 1978) pp. 16-17.

37. R. A. DeMillo, R. J. Lipton and F. G. Sayward, "Program Mutation: A New Approach to Program Testing", in E. F. Miller (editor) *Software Testing, Volume 2: Invited Papers,* Infotech International, 1979, pp. 107-128. [Volume 1 on this work contains helpful analysis and bibliography].

38. R. A. DeMillo and R. E. Miller, "Implicit Computation by Synchronization Primitives", *Information Processing Letters,* Vol. 9, No. 1 (20 July 1979) pp. 35-38.

39. R. A. DeMillo and D. P. Dobkin, "Recent Progress in Secure Computation", *Proceedings 1978 IEEE COMPSAC* (November 1978) Chicago, Illinois.

40. R. A. DeMillo and R. J. Lipton, "Some Connections between Computational Complexity and Mathematical Logic", *Proceedings 11th ACM Symposium on Theory of Computing* (May 1979) Atlanta, Georgia, pp. 153-159.

41. R. A. DeMillo, R. J. Lipton and A. J. Perlis, "Social Processes and Proofs of Theorems and Program", *Communications of the ACM*, Vol. 22, No. 5 (May 1979) pp. 271-280. [See also correspondence in "ACM Forum", *Communications of the ACM*, vol. 22, No. 11 (November 1979); an earlier version of this paper was published in the proceedings of the *6th ACM Symposium on Principles of Programming Languages* (January 1977) Santa Monica, California, pp. 245-262; This paper has been reprinted under the same title many times. It has appeared in *The Mathematical Intelligencer*, January, 1981, the 1984 anthology *Mathematics: People Problems, Results*, edited by D. C. Campbell and J. C. Higgins, published by Wadsworth International, the 1987 anthology *Currents in the Philosophy of Mathematics* edited by Thomas Tomasczko, the 1998 revised version which appeared under the title *New Directions in the Philosophy of* and the 1993 anthology *Program Verification*, edited by Timothy R. Colburn, James H. Fetzer and Terry L. Rankin, published by Kluwer Academic Publishers. This paper appeared as one of the 46 most influential papers in the history of computer science in "Ideas that Created the Future: Classic Papers in Computer Science,:" (Harry R. Lewis editor), MIT Press, 2020 (Ideas That Created the Future | The MIT Press)

42. R. A. DeMillo, S. C. Eisenstat and R. J. Lipton, "Space-Time Tradeoffs in Structured Programming: An Improved Combinatorial Embedding Theorem", *Journal of the ACM*, Vol. 27, No. 1 (January, 1980) pp. 123-127.

43. R. A. DeMillo and R. J. Lipton, "The Consistency of P=NP and Related Problems with Fragments of Number Theory", *Proceedings 12th ACM Symposium on Theory of Computing* (May 1980) Los Angeles, California, pp. 45-57.

44. R. A. DeMillo, "New Approaches to Program Testing", *IEEE Computer*, Vol. 12, No. 3 (March 1979) pp. 105-106.

45. R. A. DeMillo, "Data Base Security" in Issues *in Data Base Management*, H. Weber and A. Wasserman (eds.), North-Holland 1979, pp. 253-256.

46. R. A. DeMillo, R. J. Lipton and R. E. Miller, "Stochastic Synchronization," 1981 *Johns Hopkins Conference on Computer Systems and Sciences*, March 1981.

47. G. I. Davida, R. A. DeMillo, R. J. Lipton, "Sharing Cryptographic Keys," *Proceedings 1980 IEEE Symposium on Security and Privacy*, April 1980, Berkeley, California.

48. R. A. DeMillo and R. J. Lipton, "A System Architecture to Support A Verifiably Secure Multilevel Security System," *Proceedings 1980 IEEE Symposium on Security and Privacy*, April 1980, Berkeley, California.

49. T. A. Budd, R. A. DeMillo, R. J. Lipton and F. G. Sayward, "Theoretical and Empirical Results in Program Testing," *Proceedings Ninth ACM Symposium Principles of Programming Languages*, Las Vegas, Nev., January 1980, pp. 181-196.

50. R. A. DeMillo and F. G. Sayward, "Statistical Measures of Software Reliability," *Software Metrics*, edited by F.G. Sayward et al, MIT Press, 1981, pp. 185-202.

51. R. A. DeMillo and R. J. Lipton, "Software Project Forecasting," *Software Metrics*, edited by F.G. Sayward, et. al., MIT Press, 1981, pp. 77-94.

52. R. A. DeMillo, "Cryptographic Protocols," Presented at Meeting of American Mathematical Society, *Proceedings of Symposia in Applied Mathematics* (1981).

53. G. I. Davida, R. A. DeMillo and R. J. Lipton, "Achieving Secure Computers Through Distributed Computing", *Proceedings Third International Conference on Distributed Computing*, Paris, April 1981.

54. R. A. DeMillo, "Validating Computer Software: Two Views" *Transactions of the 1980 Annual Meeting of the American Nuclear Society*, Washington DC, November, 1980, pp. 251-252 (Invited Paper).

55. R. A. DeMillo, R. J. Lipton, and A. J. Perlis, "Social Processes and Proofs of Theorems and Programs," The *Mathematical Intelligencer*, January 1981. *Reprinted. See main entry number [39]*

56. R. A. DeMillo, N. A. Lynch, M. J. Merritt, "Cryptographic Protocols", *Proceedings, 14th ACM Symposium on Theory of Computing*, May, 1982, pp. 383-400.

57. R. A. DeMillo and M. J. Merritt, "Protocols for Data Security," *IEEE Computer*, Volume 16, Number 2, (February 1983), pp. 39-54

58. R. A. DeMillo and R. J. Martin, "Software Test and Evaluation Project: A Status Report", *NSIA National Conference on Software Test and Evaluation*, February 1-3, 1983, Washington, DC, pp. T1-T10

59. R. A. DeMillo, "Requirements for a Test and Evaluation Subenvironment of an Advanced Software Engineering Environment" Prepared by the Software Test and Evaluation Project, under Contract Number F33657-82-G-2083 to the Georgia Institute of Technology, Atlanta, Georgia 30332, April 1984

60. R. A. DeMillo, A. B. Marmor-Squires, S. T. Redwine, Jr., W. E. Riddle, "Software Engineering Environments for Mission Critical Applications - STARS Alternative Programmatic Approaches", IDA Paper #P-1788. Prepared for Office of the Under Secretary of Defense for Research and Engineering by Institute for Defense Analyses, August 1984

61. R. A. DeMillo, "Volume 2 - Software Test and Evaluation: State-of-the-Art Overview" OSD/DDT&E Software Test and Evaluation Project, Phases I and II, Final Report, submitted to the Office of the Secretary of Defense, Director Defense Test and Evaluation and the Office of the Naval Research ONR Contract Number N00014-79-C-0231, June 1983

62. R. A. DeMillo, R. J. Martin, "Volume 1 - Report and Recommendations" OSD/DDT&E Software Test and Evaluation Project, Phases I and II, Final Report, submitted to the Office of the Secretary of Defense, Director Defense Test and Evaluation and the Office of Naval Research ONR Contract Number N00014-79-C-0231, June 1983

63. K. Vairavan and R. A. DeMillo, "On the Computational Complexity of a Generalized Scheduling Problem," *Distributed Computing: Concepts and Implementations*, edited by Paul L. McEntire, John G. O'Reilly and Robert E. Larsen, published by the IEEE Press (1984). *Reprinted. See main entry number [18]*

64. R. A. DeMillo, R. A. Gagliano, R. J. Martin, and J. F. Passafiume, "Policy Recommendations for Software Test and Evaluation: System Level Test Issues", *Journal of Test and Evaluation*, January 1984, Vol. V, No. 1, pp 21-28

65. R. A. DeMillo, R. J. Lipton, and A. J. Perlis, "Social Processes and Proofs of Theorems and Programs," *Mathematics: People, Problems, Results*, edited by D. C. Campbell and J. C. Higgins, published by Wadsworth International (1984) *Reprinted. See main entry number [39]*

66. R. W. Bartlett and R. A. DeMillo, "Computer Litigation: What the Lawyer Expects and What the Expert Needs," *Computer Law: Institute of Legal Education*, July, 1986, Atlanta, GA, pp. 167-178.

67. R. A. DeMillo, "Functional Capabilities of a Test and Evaluation Subenvironment in an Advanced Software Engineering Environment" GIT-SERC-86/07.

68. R. A. DeMillo, E. H. Spafford, "The Mothra Software Testing Environment", *Proceedings 11th NASA Software Engineering Workshop*, NASA Goddard, December 3, 1986

69. E. W. Martin, R. A. DeMillo, "Operational Survivability in Gracefully Degrading Distributed Processing Systems," *IEEE Transactions on Software Engineering*, June 1986, Vol. SE-12, Number 2

70. R. A. DeMillo, et al "The Mothra Software Testing Environment System Documentation," Georgia Institute of Technology, Software Engineering Research Center, Atlanta, Georgia 30332, June 1987, GIT-SERC-87-10. (Second Revision published by The Software Engineering Research Center, Purdue University, January 1990)

71. R. A. DeMillo, D. S. Guindi, K. N. King & W. M. McCracken, "An Overview of the Mothra Software Testing Environment," Purdue University, Software Engineering Research Center, West Lafayette, Indiana 47907, August, 1987, SERC-TR-3-P

72. R. A. DeMillo, R. J. Lipton, and A. J. Perlis, "Social Processes and Proofs of Theorems and Programs," *Currents in the Philosophy of Mathematics* edited by Thomas Tomasczko (1987). *Reprinted. See main entry number [39]*

73. W. F. Applebee, R. A. DeMillo, D. S. Guindi, K. N. King, and W. M McCracken, "Using Mutation Analysis for Testing Ada Programs," *Proceedings Spring 1988 Ada Europe Conference*, Munich, FDR. (North-Holland, 1988, also appears as Software Engineering Research Center, Purdue University Technical Report SERC-TR-9-P

74. B. Choi, R. DeMillo, W. Du, and R. Stansifer, "Observing Reusable Ada Software Components - Techniques for Recording and Using Operational Histories," Purdue University, Software Engineering Research Center, West Lafayette, Indiana 47907, 1988, SERC-TR-18-P

75. R. A. DeMillo, D. S. Guindi, K. N. King, W. M. McCracken, and A. J. Offutt, "An Extended Overview of the Mothra Software Testing Environment," *Proceedings of the Second Workshop on Software Testing, Verification and Analysis*, Banff, Canada, July 1988, pp. 142-151

76. R. A. DeMillo and A. J. Offutt, "Experimental Results of Automatic Test Data Generation," *Proceedings of Portland Software Quality Conference*, September 1988

77. B. Choi, R. A. DeMillo, R. Stansifer, and W. Du, "Observation Packages for Reusable Ada Components," *Proceedings of Symposium on Empirical Foundations of Information Sciences and Systems* (October, 1988)

78. R. A. DeMillo, E. W. Krauser and A. P. Mathur, "Using the Hypercube for Reliable Testing of Large Software," Software Engineering Research Center, Research Report Number SERC-TR-24-P, August, 1988, Purdue University

79. R. DeMillo, W. Du, and R. Stansifer. 1989. An integrated software environment for reuse. In Proceedings of the conference on TRI-Ada '88 (TRI-Ada '88). Association for Computing Machinery, New York, NY, USA, 186–197. DOI:https://doi.org/10.1145/76619.76626

80. H. Agrawal, R. DeMillo, and E. Spafford, "A Process State Model to Relate Testing and Debugging," Software Engineering Research Center, Research Report Number SERC-TR-27-P, September, 1988, Purdue University

81. R. A. DeMillo, "Test Adequacy and Program Mutation," *Proceedings 1989 International Conference on Software Engineering*, May 1989, Also appears as Software Engineering Research Center, Research Report SERC-TR-37-P, Purdue University

82. B. Choi, R. A. DeMillo, E. W. Krauser, R. J. Martin, A. P. Mathur, A. J Offutt, E. H. Spafford, "The Mothra Toolset," *Proceedings 22nd HICSS*, January 1989

83. R. A. DeMillo, "Software Testing for Critical Applications: A Position Paper," *Proceedings 13th IEEE Computer Software and Applications Conference*, Orlando, September, 1989, p. 521

84. H. Agrawal, R. A. DeMillo, R. Hathaway, E. W. Krauser, R. J. Martin, and A. P. Mathur, "The Design of Mutation Operators for C", 1989 (Submitted for Publication), also appears as "Design of Mutant Operators for the C Programming Language", Software Engineering Research Center Research Report SERC-TR-41-P, Purdue University

85. R. A. DeMillo and R. J. Lipton, "Software Windtunnels: Scale Models of Software Development Projects."

86. H. Agrawal, B. Choi, R. A. DeMillo, and A. Mathur, "CIT/CAT: Two Novel Methodologies for the Design of Software Testing Tools,", 1990

87. R. A. DeMillo, E. W. Krauser, and A. P. Mathur, "An Approach to Compiler-Integrated Software Testing," Software Engineering Research Center, Research Report SERC-TR-71-P, April 1990, Purdue University

88. H. Agrawal, R. A. DeMillo and E. H. Spafford, "An Execution Backtracking Approach to Program Debugging," *IEEE Software*, May 1991, p. 21-26

89. R. A. DeMillo and R. J. Lipton, "Defining Software by Continuous, Smooth Functions," *IEEE Transactions on Software Engineering*, Vol. SE-17, No. 4, April 1991, p 383

90. R. A. DeMillo, "Progress Toward Automating Software Testing," *Proceedings of the International Conference on Software Engineering*, Austin, Texas, May 1991, Also appears as Software Engineering Research Center Report Number SERC-TR-101-P, July, 1991, Purdue University

91. Richard DeMillo and Aditya Mathur, "On the Use of Software Artifacts to Evaluate the Effectiveness of Mutation Analysis for Detecting Errors in Production Software," *Thirteenth Minnowbrook Workshop on Software Engineering*, (also Software Engineering Research Center Report Number SERC-TR-92-P, March, 1991, Purdue University)

92. R. DeMillo, E. Krauser and A. Mathur, "Compiler-integrated program mutation," in *1991 The Fifteenth Annual International Computer Software & Applications Conference*, Tokyo, Japan, 1991 pp. 351-356., doi: 10.1109/CMPSAC.1991.170202

93. R. A. DeMillo and A. J. Offutt, "Constraint-Based Test Data Generation," *IEEE Transactions on Software Engineering*,, Vol. SE-17, Number 9, September, l991, pp. 900-910

94. Hiralal Agrawal, Richard A DeMillo and Eugene H. Spafford, "Dynamic Slicing in the Presence of Pointers and Records," *Proceedings Fifth Symposium on Testing Analysis and Verification*, October, 1991, Victoria BC, pp. 60-73. (also appears as: Hiralal Agrawal and Richard DeMillo, "Dynamic Slicing in the Presence of Unconstrained Pointers," Software Engineering Research Center Report Number SERC-TR-93-P, March, 1991, Purdue University)

95. R. A. DeMillo, E. W. Krauser, and A. P Mathur, "Compiler Support for Program Testing on MIMD Architecture, *Proceedings Ninth Annual Pacific Northwest Software Quality Conference*, October, 1991, Portland, Oregon

96. R. A. DeMillo and A. J Offutt, "Experimental Results from an Automatic Test Data Generator" *ACM Transactions on Software Engineering and Methods.* Vol. 2 No. 2, April 1993, pp. 109-127

97. R. A. DeMillo, M. Furst, and R. J. Lipton, "Competitive Strategies for k Servers"

98. H. Agrawal, R. A. DeMillo and E. H. Spafford, "Debugging with Dynamic Slicing and Backtracking," *Software Practice & Experience*, June 1993, Vol. 23 No. 6, pp. 589-616

99. R. A. DeMillo, "A Defense of Incremental Research," *International Perspectives on Software Engineering*, June, 1993, Vol. 1, No. 2, pp. 33-36

100. R. A. DeMillo, R. J. Lipton, and A. J. Perlis, "Social Processes and Proofs of Theorems and Programs," *Program Verification* , edited by Timothy R. Colburn, James H. Fetzer, and Terry L. Rankin and published by Kluwer Academic Publishers (1993).*Reprinted. See main entry number [39]*

101. R. A. DeMillo, T-C Li and A. P. Mathur, "A Two Dimensional Scheme to Evaluate the Adequacy o f Fault Tolerance Testing," In Third IEEE International Workshop on Integrating Error Models with Fault Injection, pp. 54-56, Annapolis, MD, April, 1994

102. R. A. DeMillo, A. P. Mathur, and E. W. Wong, "Some Critical Remarks on a Hierarchy of Fault Detecting Abilities for Program Testing," IEEE Transactions on Software Engineering, 1995

103. R. A. DeMillo, "A Simple Architectural Rule for Conservatively Allocating Software Reliability Requirements,"

104. R. A. DeMillo, "Testability in Software Architectures: Some Definitional Suggestions"

105. R. A. DeMillo and M. Young, "Non-Functional Aspects of Software Architecture Design", Proceedings Workshop on Software Architectures, 17th International Conference on Software Engineering, Seattle, Washington, April 1995, pp. 72-79

106. R. A. DeMillo, "Scalability in Software Architectures"

107. R. A. DeMillo and M. Young, "Quantitative Aspects of Software Architecture" Proceedings of the 15th Annual Software Technology Conference, Salt Lake City, Utah, April, 1995

108. R. A. DeMillo and D. I. Hmeljak, "C_{pk} Calibration of the Capability Maturity Model"

109. R. A. DeMillo and R. J. Lipton, "A Gang of Ten Problems in Formal Methods" (unpublished manuscript), 1994 *An earlier version of this paper was presented by the first author at the 1990 ACM Symposium on Test, Analysis and Verification, Victoria, BC*

110. A. Apostolico, G-F. Bilardi, F. Bombi and R. A. DeMillo, "An International Masters Program in Software Engineering: Experience and Prospects" Proceedings 11th Data Engineering Conference, Taipei, Taiwan, March 1995

111. R. A. DeMillo, T-C Li, A. P. Mathur, "Using a Hierarchical Failure Mode Set to Assess the Adequacy of Test for Fault-Tolerance," Fourth IEEE International Workshop on Evaluation Techniques for Dependable Systems, 1995

112. R. A. DeMillo, H. Pan, and E. H. Spafford, "Critical Slicing" Proceedings 1996 ACM International Symposium on Software Test and Analysis, San Diego, California, pp. 121-134, January 1996

113. R. A. DeMillo, "Mission-Critical Applications, Commercial Value and Software Quality", ACM Symposium on Strategic Research Directions (June 1996) Boston, Massachusetts.

114. D. Boneh, R. DeMillo and R. J. Lipton, "Encrypted Quantum Measurement" (unpublished manuscript, 1996)

115. L. Osterweil, L. Clarke, R. A. DeMillo, S. F. Feldman, W.McKeeman, E, Miller and J. Salasin, "Strategic Directions in Computing: Software Quality", Symposium on Strategic Research Directions (June 1996) Boston, Massachusetts.

116. R. DeMillo and R. J. Lipton, "Critique of Formal Verification: Alan Perlis and the Seeds of Method and Doubt", in *In the Beginning: Personal Recollections of Software Pioneers* (R. L. Glass, editor) IEEE Computer Society Press (to appear)

117. D. Boneh, R. DeMillo and R. J. Lipton, "On the Importance of Checking Computations" *Eurocrypt 97*, Springer-Verlag, Heidelberg, May 1997

118. R. DeMillo, H. Pan and E. Spafford, "Failure and Fault Analysis for Software Debugging," *Proceedings IEEE COMPSAC*, 1997.

119. R. DeMillo, "The Internet as a Telephone Network", *Educom Review,* Jan/Feb 1998, pp. 12-16.

120. R. A. DeMillo, R. J. Lipton, and A. J. Perlis, "Social Processes and Proofs of Theorems and Programs," *New Directions in the Philosophy of Mathematics* edited by Thomas Tomasczko (Revised and Expanded Edition, 1998), Princeton University Press, pp. 267-286 *Reprinted. See main entry number [40]*

121. D. Boneh, R. A. DeMillo and R. J. Lipton, "On the Importance of Eliminating Errors in Cryptographic Computations, *Journal of Cryptography 14 (2001) 2, 101-119.* See main entry [115]. This paper has been cited many times. It resulted in a revision to the Open SSL Toolkit (rev 0.9.7) requiring a check of the RSA-CRT result.

122. R. A. DeMillo and R. J. Lipton, "Social Processes and Proofs: A Quarter-Century Perspective," Presented to the Royal Society of London, October, 2004.

123. R. C. Basole and R. A DeMillo, "Information Technology" in *Enterprise Transformation* (edited by W. C. Rouse) Wiley, 2006

124. Richard A. DeMillo, "Keeping Technology Promises," *Communications of the ACM*, November 2012 (Volume 55, No. 11): 37-40.

125. P. M. A. Baker, K. R. Bujak, and R. A. DeMillo, "The Evolving University: Disruptive Change and Institutional Innovation," *Procedia Computer Science*, 14, pp. 330-335.

126. Richard A. DeMillo, "Unbundling Higher Education," in *MOOCs and Open Education Around the World* (edited by Curtis J. Bonk, Mimi Miyoung Lee, Thomas C. Reeves, and Thomas Reynolds) Routledge, 2015.

127. Rafael L. Bras and Richard A. DeMillo, "Leadership Challenges in Higher Education's Digital Future," in *Challenges in Higher Education Leadership*, (edited by James Soto Anthony, Ana Marie Cauce, and Donna Shalala), Routeledge, 2017.

128. DeMillo, Richard and Kadel, Robert and Marks, Marilyn, What Voters are Asked to Verify Affects Ballot Verification: A Quantitative Analysis of Voters' Memories of Their Ballots (November 23, 2018). Available at SSRN: https://ssrn.com/abstract=3292208 or http://dx.doi.org/10.2139/ssrn.3292208

129. Appel, Andrew and DeMillo, Richard and Stark, Philip, Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters (April 21, 2019). Available at SSRN: https://ssrn.com/abstract=3375755

130. Appel, Andrew and DeMillo, Richard and Stark, Philip, Ballot-Marking Devices Cannot Assure the Will of Voters, *Election Law Journal,* June, 2020 https://www.liebertpub.com/doi/10.1089/elj.2019.0619